

WaTech SSL VPN

End User Guide

WaTech Edition

Version 1.4
October 27, 2015



Created by:
Andrew Haines WaTech ESS Technical Lead
Jennifer Somnis Enterprise Projects Manager

Document Revision History

Description of Change	Page or Section	Date Revised	Reviser
Published first draft	All	3/31/15	Andrew Haines
Revision 1.1	All	3/26/15	Andrew Haines
Revision 1.2	All	3/31/15	Tim Gill
Revision 1.3	All	3/31/15	Phil Davis
Revision 1.4	All	10/23/15	Alex Tomita

Contents

Document Revision History	2
Introduction and Purpose	4
Device Set-Up	4
<i>Agency Workstations</i>	4
<i>Personal Workstations and Devices</i>	4
How to Log-On.....	5
The WebTop	7
How to Connect	8
How to Disconnect from Network Access.....	10

Introduction and Purpose

The purpose of this End User Guide is to provide end user training information to assist WaTech customers in planning for successful use of the WaTech SSL VPN Service. This guide will offer information about, how to log-on, initial set-up for personal devices and how to connect.

Device Set-Up

Each agency has different policies around the devices which are, or are not, allowed to VPN into their environments. Please ensure that users are following agency appropriate connection requirements before trying to use the SSL VPN service. The SSL VPN service supports a number of different devices and operating systems. However these options may be limited based upon agency specific policies.

Agency Workstations

Workstations and devices owned by Washington State agencies must have all the necessary plug-ins deployed prior to connecting through the VPN. WaTech will configure and provide agency specific plug-ins during the initial deployment. The plug-ins may be implemented by each agency to run automatically in the background without user impact. If a user has issues with first time connectivity, the user should contact the agency Help Desk to make sure the plug-ins installed successfully.

***NOTE:** Recommended browsers are Internet Explorer, Safari and Firefox. There is limited feature support with Chrome due to browser restrictions. See the [compatibility matrix](#).

Personal Workstations and Devices

If a user is allowed by agency policy to use a personal workstation or device, the user will be required to have Administrative rights on the machine and manually download and install all plug-ins. The first step for a user is to ensure that the device's operating system and browser version is compatible with the WaTech SSL VPN Service. Please check the [compatibility matrix](#) to ensure the device is supported. If the device or the version is not supported, the user should contact the agency Help Desk.

During the SSL VPN logon process the user will be prompted various times to install and allow plug-ins to run on their machine. This may require the browser to be restarted, as well as the workstation. Once the plug-ins are installed, the user shouldn't be prompted to install plug-ins again.

***NOTE:** Recommended browsers are Internet Explorer, Safari and Firefox. There is limited feature support with Chrome due to browser restrictions. For Windows 10 connectivity, Internet Explorer 11 is the only current browser that is supported. See the [compatibility matrix](#).

How to Log-On

Each agency will be supplied a specific URL for their agency. Users can also get to the link by going to the following URL <https://accesswork.wa.gov/> and selecting your agency from the landing page.

Non-Eclient WaTech Users – [Washington Technology Solutions](#)

Eclient WaTech Users – [Department of Enterprise Services](#)

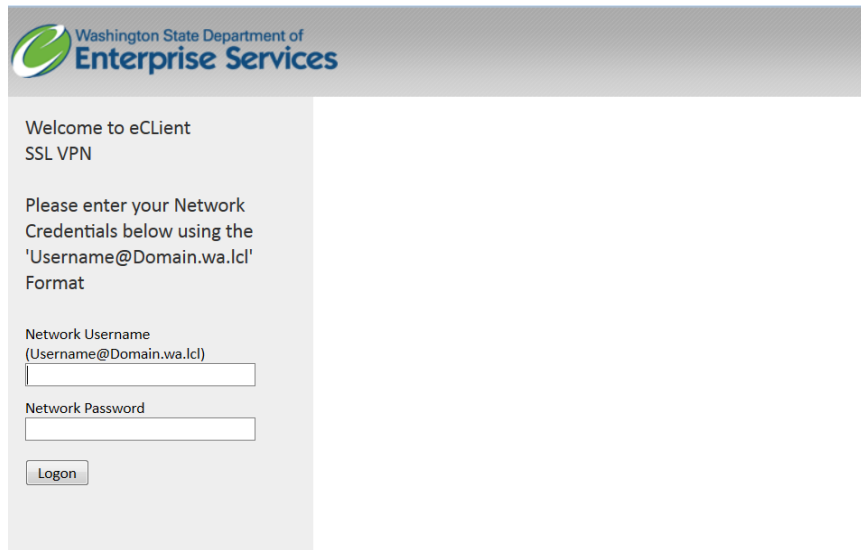
Once the user has selected the appropriate agency from the list, they will be redirected to the logon screen:

Non-Eclient WaTech Users



The screenshot shows the logon interface for Non-Eclient WaTech Users. At the top is a header with the 'WaTech' logo and the text 'Washington Technology Solutions'. Below the header, the text 'Secure Logon for WaTech' is displayed. There are two input fields: 'Username' and 'Soft-Token Passcode or KeyFob PIN + Token'. A 'Logon' button is located below the second input field.

Eclient WaTech Users

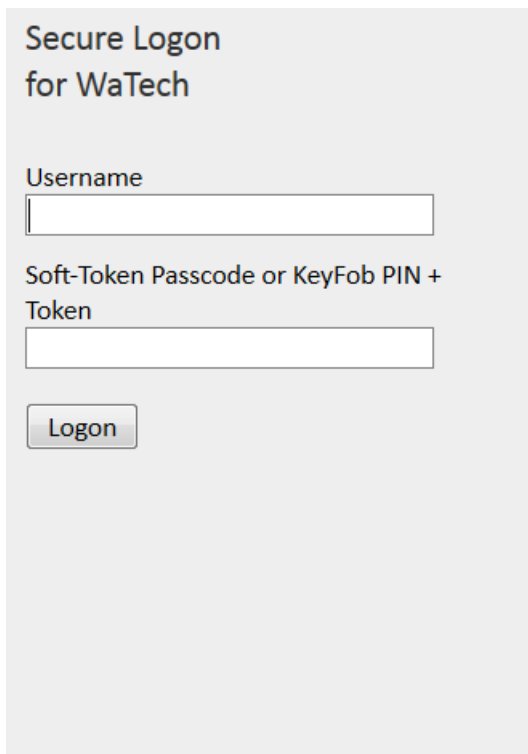


The screenshot shows the logon interface for Eclient WaTech Users. At the top is a header with the 'Washington State Department of Enterprise Services' logo. Below the header, the text 'Welcome to eClient SSL VPN' is displayed. A message states: 'Please enter your Network Credentials below using the 'Username@Domain.wa.lcl' Format'. There are two input fields: 'Network Username (Username@Domain.wa.lcl)' and 'Network Password'. A 'Logon' button is located below the second input field.

***NOTE:** Each agency's logon screen will look different. Additionally, users from another agency will **not** be able to login to another agencies VPN service.

Depending on your logon page, users will be prompted to enter one of the following:

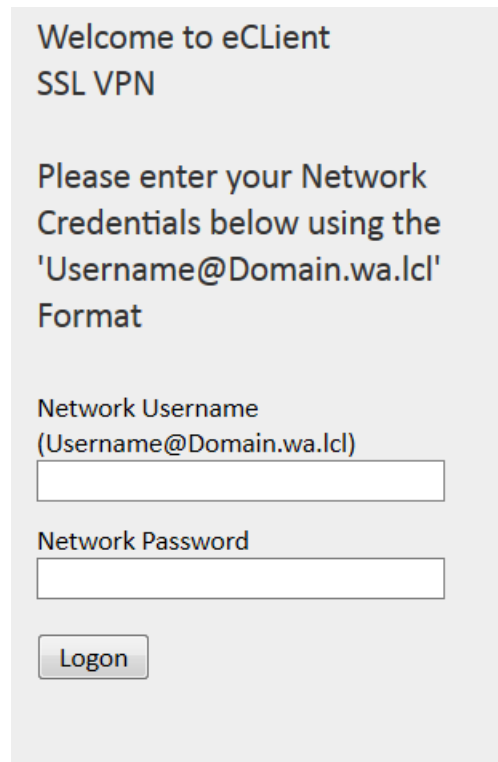
- VPN login and the RSA soft token code
- VPN login and your PIN + RSA hard token code
- Your EAD Login and Password



Secure Logon
for WaTech

Username

Soft-Token Passcode or KeyFob PIN +
Token



Welcome to eClient
SSL VPN

Please enter your Network
Credentials below using the
'Username@Domain.wa.lcl'
Format

Network Username
(Username@Domain.wa.lcl)

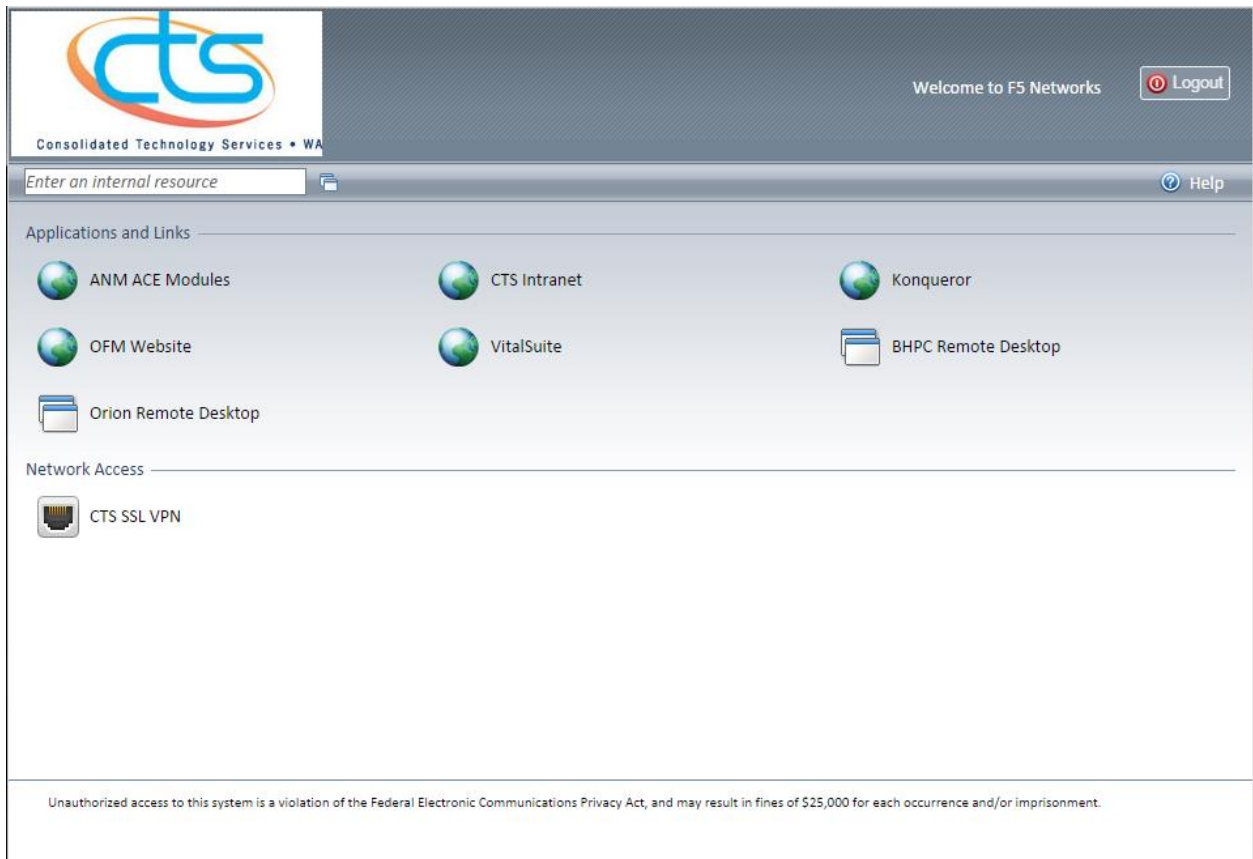
Network Password

***NOTE:** If you encounter any issues with your PIN, please submit a ticket to your agency Help Desk.

The WebTop

After a user successfully authenticates through the logon Screen, they will be presented with a WebTop. A WebTop is a container used to hold the resources which a user has the rights to use. Each user will potentially have different and unique resources assigned to them, meaning no two WebTops have to look the same.

An example of a WebTop is:



The WebTop consists of a couple main areas:

- **Internal Resources Search:** A search field for finding resources the agency has made available via VPN.
- **Applications and Links:** Applications and Web Hyperlinks presented to the user as configured by the VPN Administrator.
- **Network Access:** The VPN resource for users to create a full SSL tunnel into the agency network.
- **Logout Button:** Button for users to close their authenticated VPN session.
- **Help Button:** Button containing help tips.

The items within the Applications and Links section and the Network Access section are assigned to users by the agency VPN Administrator.

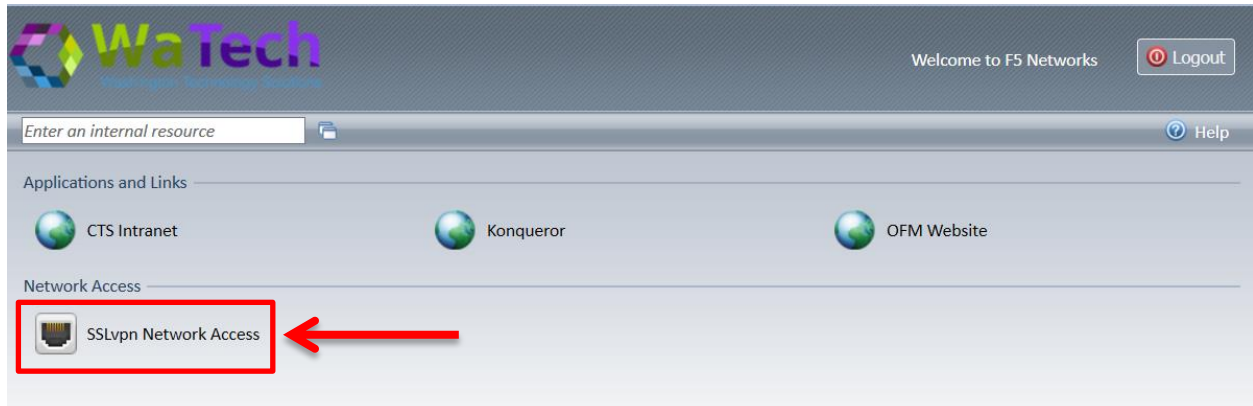
A user will click the desired resource to make it launch.

***NOTE:** If any issues are encountered trying to launch an item, please contact the Agency Help Desk.

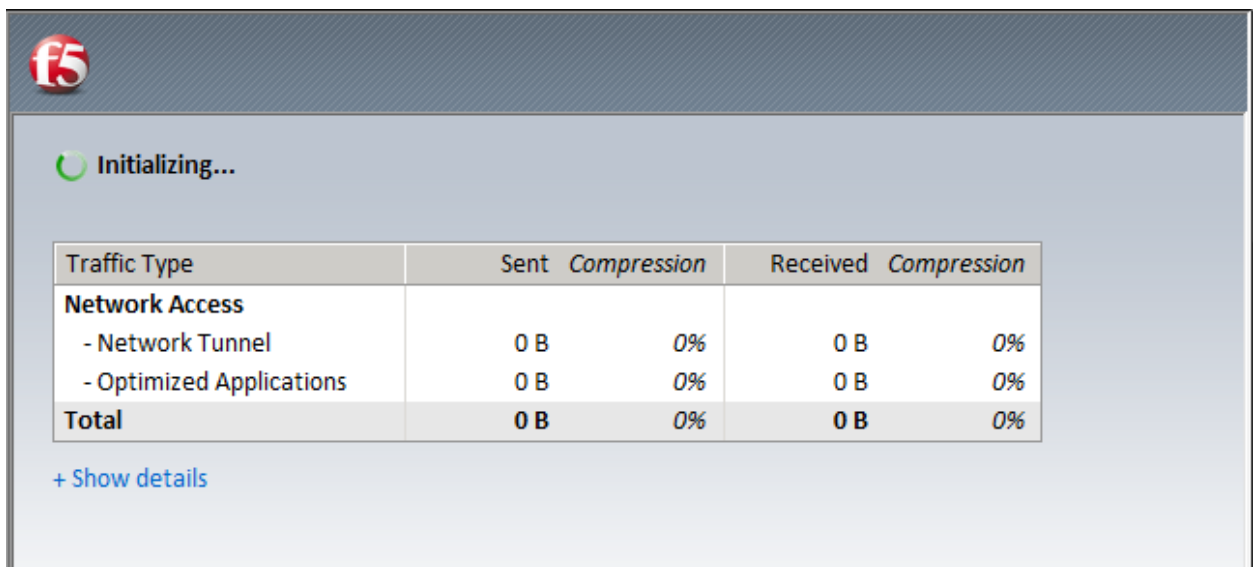
How to Connect

If a user has been granted the Network Access resource, they will have an icon on their WebTop. Once a user has authenticated into the F5 WebTop, the Network Access does not automatically launch. The user must click the item.

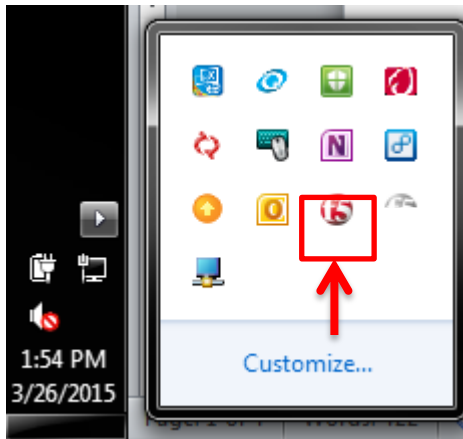
In this case, the Network Access resource is as shown below:



Once a user clicks the Network Access icon (SSLvpn Network Access in this example), they will be presented with a F5 pop-up detailing their connection status. This pop-up looks like this:



Upon successful connection, the F5 pop-up will automatically close itself and the user will be able to verify connectivity by checking the system notification tray. Within the tray, the user will have an illuminated F5 Icon showing they are connected.

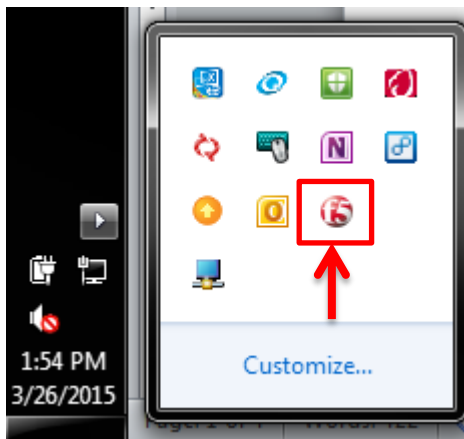


Once a user has connected using the Network Access resource, a secure connection into the agency network will be established. A user can work as if directly connected to the network in the office. This means that applications such as Outlook, Skype, SharePoint, SSH to servers etc. will all be available for use.

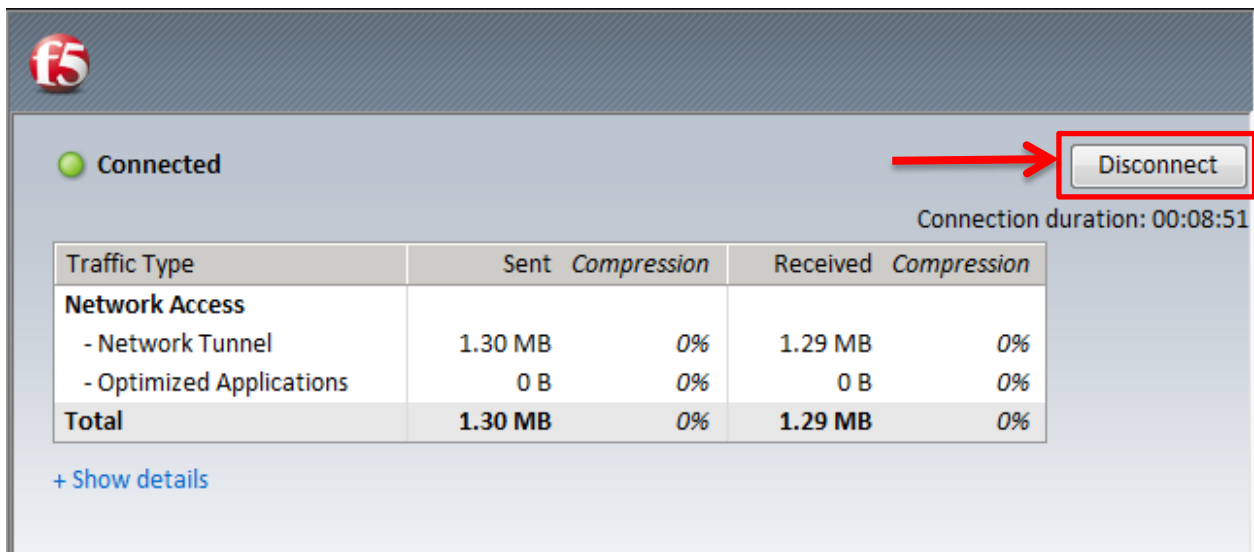
In order for a user who has connected to the VPN from a personal machine to remotely connect to an agency workstation, the workstation must be powered-on, and be connected to the network. The user will enter the workstation's Computer Name or IP Address into the Remote Desktop application and then enter their login credentials when prompted.

How to Disconnect from Network Access

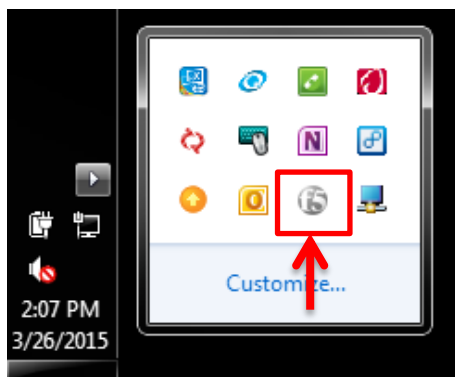
To disconnect from a Network Access VPN session, the user must first open up their system notification tray and double-click the illuminated F5 icon.



Once done, this will open up the minimized F5 pop-up showing your connection. To disconnect, simply select the 'Disconnect' button in the upper right hand corner:



Once clicked, the VPN connection into the agency network will close, the pop-up will close and the icon in the system notification tray will become grey showing that the connection is no longer in place.



How to Disconnect from the SSL VPN Service

If you want to disconnect from the SSL VPN service completely, first switch back to the browser window you originally logged in from. From there, you can click on the “Logout” button in the upper right corner to disconnect from the service.

